ABSTRACT

A method for implementing IPsec in third generation and beyond wireless, mobile access, Internet protocol-based digital networks supporting Mobile IP is disclosed. A sending node initiates establishment of a security association for a receiving node, rather than waiting for the receiving node to initiate security association establishment after receiving a packet from the sending node. Thus, the disclosed method greatly reduces packet delay introduced by required authentication and security association establishment processes. The IPsec may use the Kerberos key exchange method. The Kerberos key exchange method, since it requires less computational overhead, is a suitable IPsec method for mobile IP networks where less resourceful devices such as PDAs and cellular phones are primary network access devices. Since the Kerberos key exchange method requires less computational overhead, packet delay associated with authentication and security processes are further reduced.